Protection of Behavioural Generated Personal Data of Consumers

S Koos
Federal Republic of Germany, Universität der Bundeswehr, München

stefan.koos@unibw.de

ABSTRACT

Personal behavioural generated data are a special problematic of the Data Protection Law as they arise directly out of the intimate sphere of the individual by using smart devices in the daily life. The new General Data Protection Regulation of the European Union is aiming to protect personal data in an administrative way. However, the Basic Regulation is not reacting adequately to the growing integrating connection between person and machine. The development of Internet of Things (IoT) and Wearable Computing (WC) needs private law instruments such as contractual models or IP licensing models to give to the individual the sovereignty over his own personal data.

Keywords*: Data, Protection, Regulation*

1. INTRODUCTION

Personal data citizens are important economic goods. Their value can be measured in money as a market is existing for data. In the era of *IoT* (*`Internet of Things´*, i.e. GPS-equipped smartphones, smartwatches, smart glasses, smart loudspeakers, internet connected refrigerators, permanently connected to the internet and transferring data to companies) and *Wearable Computing*exploitable personal data are generated by the users of smart devices themselves by their daily activities and behaviour. Personal data are disclosed by the consumers using social media, communication apps and home entertainment. How should behavioural personal data of consumers be legally protected?

2. LITERATURE REVIEW

The Administrative Approach: General Data Protection Regulation of the European Union

Since May 25 2018 the EU General Regulation on Data Protection (GDPR, *Regulation [EU] No. 2016/279 of April 26 2016*) is applied. Art. 1 of the Regulation defines the subject matter as follows:

(1) This regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

WoMELA-GG 2019, January 26-28, Medan, Indonesia

DOI 10.4108/eai.26-1-2019.2283267

(2) This regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

Remarkable is the territorial scope of the Regulation as it is extraterritorial. The Regulation therefore applies also to the processing of personal data outside the European Union as far as personal data of data subjects within the European Union and if its connected with the chargeable or complimentary offering of goods or services or with the observation of the behaviour of persons within the European Union (Art. 2).

The legislative procedure was accompanied by activities of lobbying groups, namely of the US-government same as US-American IT-companies and other technology companies. The data protection standard in the USA is relatively low and especially US-companies awaited a "*California-Effect*" of the Regulation, a term which refers to the factual raising of protection standards within the entire USA as effect of the strict Californian environmental laws.

The Regulation is not changing the basic principles of data protection as they were already before regulated in Europe, such as *data avoidance* and *data reduction*, *purpose limitation*, *ban subject to permit* and *data transparency* (Art. 5 and 6). Basically, those principles are not new; never theless the applicability of the Regulation led to a remarkable unrest under companies and organizations who are processing data. The reason of this is the widening of the organizational requirements by the Regulation which are not only addressing companies but equally authorities, educational institutes or small private associations and clubs. It imposes a considerable duty of monitoring and controlling the processing of personal data and of the implementation of appropriate data protection policies. Controllers must be able to proof the compliance with the data protection rules of the Regulation for example by proving the existence and compliance with approved codes of conducts or approved certification mechanisms (Art. 24, Art. 40). Responsible persons must implement adequate technical and organizational measures to enforce the basic principles of data protection (*privacy by design*). Examples are the pseudonymization or measures, which ensure *by default* that only data are stored that are necessary for the specific purpose of the processing. It must be ensured that *by default* personal data are not made accessible to other persons without the intervention of the individual (Art. 25; *privacy by default*). Foreign based controllers or processors have to designate a representative established in the EU.

A problem couldbecome the duties of information to the data subject and the requirement of a consent by the individual with the procession. Persons have to be informed about all important aspects of the data processing, namely about the specific purpose of the data collection, the legitimate interests of the processing or the intention to transfer personal data to a third country or international organization (Art. 13, Art. 45, 46).Within the public discussion in Europe this is recently considered a major obstacle to the work of small private organizations and associations. However, the duties are not entirely different compared with the legal situation so far. For example, the formal requirements for the consent of the individuum are lower, compared to the national German Data Protection Act, as the written form is not always required for the consent.But as the sanctions for infringements against the provisions of the Regulation are extremely severe (up to 20 Mio EUR or up to 4 % of the worldwide turnover compared to 300.000 EUR in the national German Data Protection Act) and as the burden of proof regarding the compliance hits the companies, authorities and associations, the consequences of the application of the new law are widely feared. The Regulation is applied to many entities which before were not addressees of data protection law. Furthermore, entities are responsible for the processing or deleting of personal data not only in their own systems but also in the systems of external processors.

3. RESULT AND DISCUSSION

The Private Law `Assignment Content´ of Self-Generated Personal Data – Who is the `Owner` of IoT-Data?

The legislative approach of the GDPR is not dealing with the civil law dimension of the data protection. The Regulation ignores specific problems of the connection of the individual with the internet which will come up even more with the development of augmented reality and the connection between human and technical device. Who is the owner of behavioural generated personal data? If personal data which can be economically exploited by companies are generated by the person itself it seems on the first view evident, that the data protection law should not be limited to an administrative ´defensive` purpose but should be expanded to a private law `property´ purpose.

It is not obvious that the `assignment content´ of commercially exploitable personal data should be on the commercial user, the producer of the smart device or the processor of such data. Personal data are a relevant market object. The economic value of personal data could be considered as assigned to the individual just because of the fact that they are connected with the individual and its personality. Referring to this the interest of the person arising from the protection of the own personality may be already sufficiently fulfilled by the administrative protection of the GDPR which is basically `defensive`.

However, the aspect that some especially valuable data are generated by the own activities of the person leads to the idea, that they are goods which are produced by someone – the consumer – and the producer of a good should be the owner of it and entitled to economically exploit the good. Referring to the civil law theory of property containing the functions of the owner's *right of defence* (the *negative* function) and the owner's *right to use or not use* the good (the *positive* function) it should be considered how the positive function of the ´ownership` of personal data could be effectively protected. Possible concepts must also integrate considerations on the trade and transfer of the good and adequate reimbursement concepts.

On the other side a possible counter position to this may be, that behavioural generated personal data are `mined´ within the personal sphere of the consumer by using the smart device, but its `*refining process´* is done on the side of the company who produces or operates the smart device or service. The data are practically not usable for the consumer himself. Thus, the reason – the relevant ´investment` - for a property protection would not be the basic data generating process by the consumer but rather the technical and logistic *data refining process*.

In the Economic Analysis of Law, we find the approach that resources should be allocated following the idea of social efficiency. If we take into consideration that those data are useless in the hand of the consumer, who is not able to do the `*refining process´* himself, a more efficient allocation could be the contribution of an intellectual property right to the operator who does the `refining work´. An effective protection of the consumer´s interest in not being infringed by the commercial exploitation of his personal data could be sufficiently done by administrative rules such as the GDPR (which should be adapted more to the specific problems of IoT).The defensive interest of the consumer may be secured by giving the consumer a *veto right*, which can inhibit the creation of an Intellectual Property Right at the operator or producer of IoT-devices [1].

If on the other hand we contribute the assignment content of IoT-Data to the consumer as bearer of his Personal Rights, acknowledging the `*mining process´* of the raw data by using

smart devices as the relevant aspect to contribute a property-like right to the consumer, then we can differentiate between a pure intellectual property approach and a rather contractual approach.

The contractual approach sees the relationship between the user of smart devices or services and the producer or service provider as a mutual relation. In 2015 the EU-Commission was presenting a proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content [2]. Within the discussion on this proposal there is also the idea, that i.e. in cases, when consumers have to allow the disclosure of personal data in order to use a device or service, the personal data should be considered as "*counter performance*" of the contract.

In this concept the consumer pays the service with money and additionally with his data or – in case of complimentary services such as Facebook – exclusively with his data (see Art. 3 (1), 15 (2b), 16 (4a) of the Proposal). This approach must be carefully equilibrated with the fact that personal data are inseparable connected with the personality of the consumer, thus it is subject to the protection of the EU-Charter of Fundamental Rights [3].

A second approach is the acknowledgement of an Intellectual Property Right *sui generis* of the consumer referring to his behavioural generated personal data. This approach is differentiating between the subject matter of the data protection law (*person-related data*) and the subject matter of a *`Data Property Law´*(*behavioural generated data*) [4]].The legal subject is acquiring an *`intangible law functional property´* of behavioural generated information-data as a user in digital spaces [4]. This idea aims primary at a power of the citizen to execute influence to digital law regulatory areas and to the design of user and marketing arrangements [4]. It is the idea of protecting of the personality interests by using intellectual property rights instruments.

4. CONCLUSION

The pure administrative approach by fining misuse of personal data in its recent state is not sufficient to protect the interest of the consumer in the IoT. The concept of an *`opt-in´* which can be given conclusively by the user of smart devices is not adequate to the permanent and subliminal character of permanently data transferring smart devices. A private law enforcement generally can be effective in the fight against infringements of protection rules. Preferable is an approach which makes the consumer the owner of its personal behavioural generated data, as it gives the consumer a legally developed sovereignty against commercial users of his data, protecting his personal rights. Objections against the commercialization of personal rights were always raised as it is now the case against the commercialization of personal data.

However, parts of the personality are already factually established as trade goods and the law should provide solutions to this economic reality. Dogmatic concepts are available, which accept the tradability of personal rights aspects but at the same time retain the connection between those aspects and the person, giving the person control sovereignty against the economical exploitation. The acceptance of a fungible property position of personal data does not necessarily mean an infringement of the constitutional concept of the human dignity.

The approach of the contribution of an Intellectual Property Right only to the producer of smart devices may be economically persuading as consumers are basically not able to use the data themselves. Therefore, an Intellectual Property Right of the consumer would have merely the purpose of being transferred or licensed by the consumer to companies with the ability to

refine and to use the data [1]. This approach seems too strong focusing on economical effectiveness and ignoring the function of property rights as defensive instruments within the personality rights protection system. The Copyright has also a defensive purpose in favour of the personality rights interest of the individual. It is the consumer him self who generates the data with his behaviour and the need to be protected in his interests arising from the personality right is hindering an assignment of an IPR to the IT-enterprise by the pure reason of the `*refining process´* and of economical effectiveness.

The opinion, which assigns an IPR of behavioural generated personal data to the consumer as the producer of the data is well comprehensible. The concept is giving the sovereignty of control of the use of those data to the consumer in the interest of his own personal rights. A practical concept of economical use of such data can be implemented by the idea of licenses. Economical use of the data can be remunerated individually in the sense of license fees or in a collective way i.e. by collecting societies or other adequate methods [4].

REFERENCES

[1] B. M, *Schutzrechte an Maschinendaten und die Schnittstelle zum Personendatenschutz Festschrift für Karl-Heinz Fezer ed W Büscher et al*. Munich: C.H.Beck, 2016.

[2] E. Council and Council of the European Union, "New rules for contracts for the supply of digital content - Council adopts its position," *European Council Council of the European Union*, 2015. [Online]. Available: https://www.consilium.europa.eu/en/press/press-releases/2017/06/08/contracts-for-digital-content-supply/.

[3] European Data Protection Supervisor, "Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content," Brussels, 2017.

[4] K.-H. Fezer, *Dateneigentum der Bürger Zeitschrift für Datenschutz*. Berlin: Konrad-Adenauer-Stiftung, 2017.